



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **09326166 A**(43) Date of publication of application: **16 . 12 . 97**

(51) Int. Cl.

G11B 20/10
G09C 1/00
H04L 9/08

(21) Application number: **08144460**(22) Date of filing: **06 . 06 . 96**(71) Applicant: **MITSUBISHI ELECTRIC CORP**

(72) Inventor: **SAKAI YASUYUKI**
YAMAGISHI ATSUHIRO
TAKEDA EISAKU

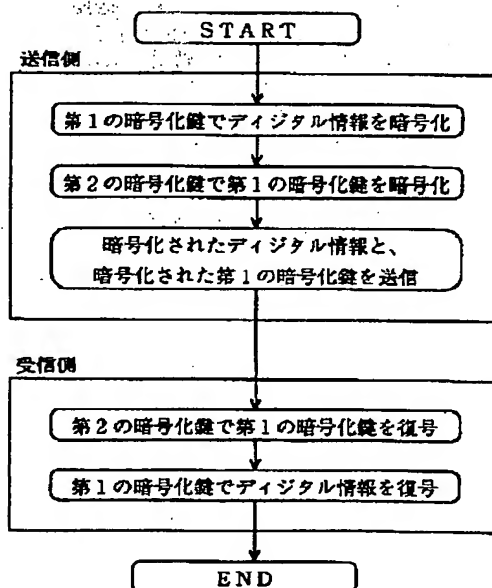
(54) **METHOD AND SYSTEM FOR PROTECTING COPYRIGHT**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a copyright protection method capable of protecting a right of an author.

SOLUTION: In a transmission side of digital information, the digital information is ciphered by a first ciphering key, and the first ciphering key is ciphered by a second ciphering key. Then, the ciphered digital information is added with the ciphered first ciphering key to be transmitted. Then, in the receiving side of the digital information, the ciphered first ciphering key is deciphered by the second ciphering key, and the ciphered digital information is deciphered by the first ciphering key obtained by the result of the deciphering.

COPYRIGHT: (C)1997,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-326166

(43) 公開日 平成9年(1997)12月16日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 1 1 B 20/10		7736-5D	G 1 1 B 20/10	H
G 0 9 C 1/00	6 3 0	7259-5 J	G 0 9 C 1/00	6 3 0 D
		7259-5 J		6 3 0 A
H 0 4 L 9/08			H 0 4 L 9/00	6 0 1 D
				6 0 1 A
審査請求 未請求 請求項の数10 O L (全 7 頁)				

(21) 出願番号 特願平8-144460

(22) 出願日 平成8年(1996)6月6日

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 酒井 康行

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72) 発明者 山岸 篤弘

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72) 発明者 竹田 栄作

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

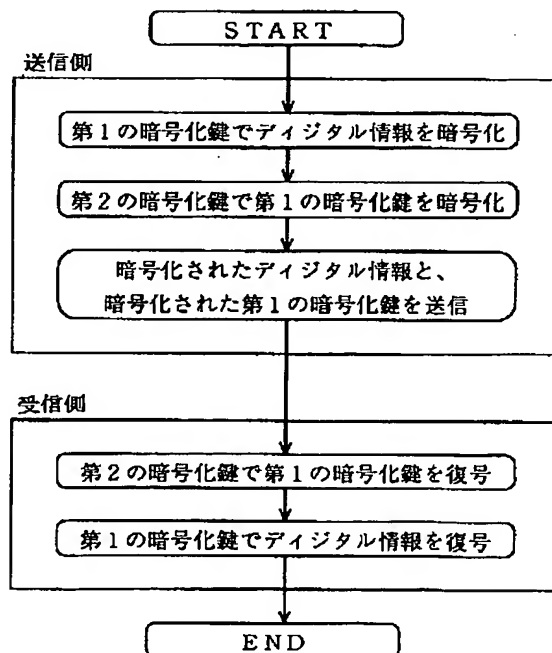
(74) 代理人 弁理士 宮田 金雄 (外3名)

(54) 【発明の名称】 著作権保護方法及び著作権保護システム

(57) 【要約】

【課題】 著作権者の権利を保護できる著作権保護方法を得る。

【解決手段】 デジタル情報の送信側において、前記デジタル情報を第1の暗号化鍵で暗号化するステップと、第2の暗号化鍵で前記第1の暗号化鍵を暗号化するステップと、前記暗号化されたデジタル情報に前記暗号化された第1の暗号化鍵を付加して送信するステップとを備え、前記デジタル情報の受信側において、前記第2の暗号化鍵を用いて前記暗号化された第1の暗号化鍵を復号するステップと、この復号の結果得られた第1の暗号化鍵を用いて前記暗号化されたデジタル情報を復号するステップとを備えたものである。



【特許請求の範囲】

【請求項1】 デジタル情報の送信側において、第1の暗号化鍵で前記デジタル情報を暗号化するステップと、第2の暗号化鍵で前記第1の暗号化鍵を暗号化するステップと、前記暗号化されたデジタル情報に前記暗号化された第1の暗号化鍵を付加して送信するステップとを備え、

前記デジタル情報の受信側において、前記第2の暗号化鍵を用いて前記暗号化された第1の暗号化鍵を復号するステップと、この復号の結果得られた第1の暗号化鍵を用いて前記暗号化されたデジタル情報を復号するステップとを備えたことを特徴とする著作権保護方法。

【請求項2】 前記第2の暗号化鍵として、前記デジタル情報の送信側と受信側のそれぞれであらかじめ保持した暗号化鍵を用いることを特徴とする請求項1に記載の著作権保護方法。

【請求項3】 前記第2の暗号化鍵として、前記デジタル情報の送信側及び受信側とは別の装置により与えられた暗号化鍵を用いることを特徴とする請求項1に記載の著作権保護方法。

【請求項4】 以下の要素を備えた著作権保護システム。

(a) 以下の手段を備えた送信装置。

(a 1) 第1の暗号化鍵でデジタル情報を暗号化する手段；

(a 2) 第2の暗号化鍵で前記第1の暗号化鍵を暗号化する手段；

(a 3) 前記暗号化されたデジタル情報に前記暗号化された第1の暗号化鍵を付加して送信する手段。

(b) 以下の手段を備えた受信装置。

(b 1) 前記第2の暗号化鍵を用いて前記暗号化された第1の暗号化鍵を復号する手段；

(b 2) 復号の結果得られた第1の暗号化鍵を用いて前記暗号化されたデジタル情報を復号する手段。

【請求項5】 前記第2の暗号化鍵として、前記デジタル情報の送信側と受信側のそれぞれであらかじめ保持した暗号化鍵を用いることを特徴とする請求項4に記載の著作権保護システム。

【請求項6】 前記第2の暗号化鍵として、前記デジタル情報の送信側及び受信側とは別の装置により与えられた暗号化鍵を用いることを特徴とする請求項4に記載の著作権保護システム。

【請求項7】 以下の要素を備えた著作権保護システム。

(a) 以下の要素を備えた第1の装置。

(a 1) この第1の装置固有の鍵情報；

(a 2) 鍵を生成する暗号化鍵生成手段；

(a 3) 初期値を暗号化鍵として前記生成した鍵を暗号化し、この暗号化した鍵を暗号化鍵として前記鍵情報を暗号化する暗号化手段；

(a 4) 前記暗号化した鍵及び前記暗号化した鍵情報を第2の装置と第3の装置に送信する送信手段。

(b) 以下の要素を備えた第2の装置。

(b 1) 擬似乱数を生成する擬似乱数生成手段；

(b 2) 初期値を用いて前記送信された鍵を復号し、この復号した鍵を用いて前記暗号化した鍵情報を復号する復号手段；

(b 3) 前記生成した擬似乱数を暗号化鍵としてデジタル情報を暗号化し、前記復号した鍵情報を暗号化鍵として前記生成した擬似乱数を暗号化する暗号化手段；

(b 4) 前記暗号化したデジタル情報及び前記暗号化した擬似乱数を第3の装置に送信する送信手段。

(c) 以下の要素を備えた第3の装置。

(c 1) 前記第1の装置の送信手段により送信された鍵情報を復号し、この復号した鍵情報を用いて前記第2の装置の送信手段により送信された擬似乱数を復号し、この復号した擬似乱数を用いて前記第2の装置の送信手段により送信されたデジタル情報を復号する復号手段。

【請求項8】 前記第1の装置の暗号化鍵生成手段は、システムに固有の暗号化鍵を生成することを特徴とする請求項7に記載の著作権保護システム。

【請求項9】 前記第1の装置の暗号化鍵生成手段は、前記第2及び第3の装置を識別するID情報を用いて暗号化鍵を生成し、

前記第2の装置の復号手段は、前記暗号化鍵生成手段により生成された暗号化鍵を用いて前記暗号化した鍵情報を復号することを特徴とする請求項7に記載の著作権保護システム。

【請求項10】 前記第1の装置の暗号化鍵生成手段は、前記第1、第2及び第3の装置を識別するID情報を用いて暗号化鍵を生成し、前記第2の装置の復号手段は、前記暗号化鍵生成手段により生成された暗号化鍵を用いて前記暗号化した鍵情報を復号することを特徴とする請求項7に記載の著作権保護システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、データの不正な複製を防ぎ、著作権者の権利を保護できる著作権保護方法及び著作権保護システムに関する。

【0002】

【従来の技術】従来のDVD (Digital Video Disc) を再生する装置について説明する。

【0003】図3は、DVDを再生するための従来の光ディスクシステムである。図において301はDVD再生装置、302はディスク、303はCD-ROMデコーダ、304は復調回路、305は誤り訂正回路、306はマルチプレクサ、307はバスインタフェースである。DVD再生装置301はDVDとCD-ROMの両方のディスクを再生できるように構成されている。次に

動作を説明する。ディスク 302 から読み出されたデータは、CD-ROM デコーダ 303 および復調回路 304 に入力される。CD-ROM デコーダ 303 では CD-ROM の場合の復調、誤り訂正が行われる。復調回路 304 ではディスク 302 から読み出された信号をデジタルデータに復調する。復調されたデータは、誤り訂正回路 305 に入力され、DVD フォーマットのデータの誤り訂正を行う。マルチプレクサ 306 では、ディスク 302 が DVD、CD-ROM のいずれであるかに応じてデータを選択し、バスインタフェース 307 に出力する。

【0004】

【発明が解決しようとする課題】従来の DVD を再生する光ディスクシステムは、ディスクに記録されているデジタルデータを何ら加工せず、記録されているままに再生していた。そのため、ディスクに記録されているデータの複製を作ることが容易であり、データの著作権者の権利を保護することが困難であるという問題点があった。

【0005】本発明の目的は、係る問題点を解決するためになされたもので、データの複製を作ることが困難で、著作権者の権利を保護することができる著作権保護方法及び著作権保護システムを得ることにある。

【0006】

【課題を解決するための手段】本発明の請求項 1 に係る著作権保護方法は、デジタル情報の送信側において、第 1 の暗号化鍵で前記デジタル情報を暗号化するステップと、第 2 の暗号化鍵で前記第 1 の暗号化鍵を暗号化するステップと、前記暗号化されたデジタル情報に前記暗号化された第 1 の暗号化鍵を付加して送信するステップとを備え、前記デジタル情報の受信側において、前記第 2 の暗号化鍵を用いて前記暗号化された第 1 の暗号化鍵を復号するステップと、この復号の結果得られた第 1 の暗号化鍵を用いて前記暗号化されたデジタル情報を復号するステップとを備えたものである。

【0007】本発明の請求項 2 に係る著作権保護方法は、前記第 2 の暗号化鍵として、前記デジタル情報の送信側と受信側のそれぞれであらかじめ保持した暗号化鍵を用いるものである。

【0008】本発明の請求項 3 に係る著作権保護方法は、前記第 2 の暗号化鍵として、前記デジタル情報の送信側及び受信側とは別の装置により与えられた暗号化鍵を用いるものである。

【0009】本発明の請求項 4 に係る著作権保護システムは、以下の要素を備えたものである。

(a) 以下の手段を備えた送信装置。

(a 1) 第 1 の暗号化鍵でデジタル情報を暗号化する手段；

(a 2) 第 2 の暗号化鍵で前記第 1 の暗号化鍵を暗号化する手段；

(a 3) 前記暗号化されたデジタル情報に前記暗号化された第 1 の暗号化鍵を付加して送信する手段。

(b) 以下の手段を備えた受信装置。

(b 1) 前記第 2 の暗号化鍵を用いて前記暗号化された第 1 の暗号化鍵を復号する手段；

(b 2) 復号の結果得られた第 1 の暗号化鍵を用いて前記暗号化されたデジタル情報を復号する手段。

【0010】本発明の請求項 5 に係る著作権保護システムは、前記第 2 の暗号化鍵として、前記デジタル情報の送信側と受信側のそれぞれであらかじめ保持した暗号化鍵を用いるものである。

【0011】本発明の請求項 6 に係る著作権保護システムは、前記第 2 の暗号化鍵として、前記デジタル情報の送信側及び受信側とは別の装置により与えられた暗号化鍵を用いるものである。

【0012】本発明の請求項 7 に係る著作権保護システムは、以下の要素を備えたものである。

(a) 以下の要素を備えた第 1 の装置。

(a 1) この第 1 の装置固有の鍵情報；

(a 2) 鍵を生成する暗号化鍵生成手段；

(a 3) 初期値を暗号化鍵として前記生成した鍵を暗号化し、この暗号化した鍵を暗号化鍵として前記鍵情報を暗号化する暗号化手段；

(a 4) 前記暗号化した鍵及び前記暗号化した鍵情報を第 2 の装置と第 3 の装置に送信する送信手段。

(b) 以下の要素を備えた第 2 の装置。

(b 1) 擬似乱数を生成する擬似乱数生成手段；

(b 2) 初期値を用いて前記送信された鍵を復号し、この復号した鍵を用いて前記暗号化した鍵情報を復号する復号手段；

(b 3) 前記生成した擬似乱数を暗号化鍵としてデジタル情報を暗号化し、前記復号した鍵情報を暗号化鍵として前記生成した擬似乱数を暗号化する暗号化手段；

(b 4) 前記暗号化したデジタル情報及び前記暗号化した擬似乱数を第 3 の装置に送信する送信手段。

(c) 以下の要素を備えた第 3 の装置。

(c 1) 前記第 1 の装置の送信手段により送信された鍵情報を復号し、この復号した鍵情報を用いて前記第 2 の装置の送信手段により送信された擬似乱数を復号し、この復号した擬似乱数を用いて前記第 2 の装置の送信手段により送信されたデジタル情報を復号する復号手段。

【0013】本発明の請求項 8 に係る著作権保護システムは、システムに固有の暗号化鍵を生成する暗号化鍵生成手段を備えたものである。

【0014】本発明の請求項 9 に係る著作権保護システムは、前記第 1 の装置において、前記第 2 及び第 3 の装置を識別する ID 情報を用いて暗号化鍵を生成する暗号化鍵生成手段を備え、前記第 2 の装置において、前記暗号化鍵生成手段により生成された暗号化鍵を用いて前記暗号化した鍵情報を復号する復号手段を備えたものであ

る。

【0015】本発明の請求項10に係る著作権保護システムは、第1の装置において、前記第1、第2及び第3の装置を識別するID情報を用いて暗号化鍵を生成する暗号化鍵生成手段を備え、前記第2の装置において、前記暗号化鍵生成手段により生成された暗号化鍵を用いて前記暗号化した鍵情報を復号する復号手段を備えたものである。

【0016】

【発明の実施の形態】

実施の形態1．本発明による著作権保護方法の一実施の形態を図1に基づいて説明する。図1は、本実施の形態による著作権保護方法のフローチャートである。

【0017】次に動作を説明する。まず、デジタル情報の送信側と受信側とで、共通の第2の暗号化鍵を共有し、保持しておく。デジタル情報の送信側は、まず第1の暗号化鍵を用意する。次にこの第1の暗号化鍵を用いてデジタル情報を暗号化する。次に、共有し保持されている第2の暗号化鍵で第1の暗号化鍵を暗号化する。次に、暗号化されたデジタル情報に、暗号化された第1の暗号化鍵を付加して送信する。デジタル情報の受信側は、次の動作を行う。まず、共有されている第2の暗号化鍵で暗号化された第1の暗号化鍵を復号する。次に、復号された第1の暗号化鍵を用いて、デジタル情報を復号する。

【0018】以上のようにデジタル情報を暗号化して送信することにより、情報の不正な複製を防ぐことができ、情報の著作権者の権利を保護することができる。

【0019】実施の形態2．前記実施の形態1では、第2の暗号化鍵はあらかじめ送信側と受信側で共有されていたが、送信側、受信側以外の第3者が供給することもできる。

【0020】実施の形態3．本発明による著作権保護システムの一実施の形態を、図2に基づいて説明する。図2は、本実施の形態による著作権保護システムの構成図である。図において、201は第1の装置であり、例えばICカードおよびPCカードなどの携帯型情報記録媒体である。202は第1の装置201毎に固有でかつ秘密の鍵情報、203は第1の装置201を識別する第1のID情報、204は暗号化鍵を生成する暗号化鍵生成手段、205は鍵情報202を暗号化する第1の暗号化手段、206は第1の復号手段、207は第1のインタフェースである。208は第2の装置であり、例えばDVDである。209は第2のID情報、210は擬似乱数生成手段、211は第2の暗号化手段、212は第2の復号手段、213は第2のインタフェース、214はデジタル情報である。第2の装置208は、デジタル情報214を暗号化して送信する。215は第2の装置208により暗号化して送信されたデジタル情報214を受信して復号する第3の装置であり、例えばユー

ザが使用するパソコンである。216は第3のID情報、217は第3の復号手段、218は第3のインタフェース、219は第1～第3の装置にそれぞれ格納されている初期値である。

【0021】次に動作を説明する。まず、鍵情報202を、第1の装置201、第2の装置208及び第3の装置215の3つの装置で共有する手順を説明する。第1の装置201にはあらかじめ、固有の鍵情報202、第1のID情報203及び初期値219が書き込まれている。第2の装置208にはあらかじめ、第2のID情報209及び初期値219が書き込まれている。第3の装置215にはあらかじめ、第3のID情報216及び初期値219が書き込まれている。初期値219は、第1の装置201、第2の装置208及び第3の装置215において共通の値である。まず、第1の装置201の暗号化鍵生成手段204において暗号化鍵を生成し、その暗号化鍵は、第1の暗号化手段205により初期値219を暗号化鍵として暗号化され、第1のインタフェース207を介して第2の装置208及び第3の装置215に送信される。第2の装置208及び第3の装置215でそれが復号され、暗号化鍵生成手段204において生成された暗号化鍵は、システムを構成する3つの装置に固有の鍵であり、3つの装置で共有される。次に、この共有された暗号化鍵を用いて、第1の暗号化手段205において鍵情報202を暗号化し、第1のインタフェース207を介して第2の装置208及び第3の装置215に送信される。次に、第2の復号手段212及び第3の復号手段217において、暗号化された鍵情報202は復号され、鍵情報202は、3つの装置で共有される。

【0022】次に、第2の装置208のデジタル情報214を、第3の装置215に送信する手順を説明する。まず、擬似乱数生成手段210において擬似乱数を生成し、生成された擬似乱数を暗号化鍵としてデジタル情報214を暗号化する。生成された擬似乱数は、鍵情報202を暗号化鍵として第2の暗号化手段211により暗号化する。暗号化された擬似乱数と、暗号化されたデジタル情報214を、第2のインタフェース213を介して第3の装置215に送信する。第3の装置215では、共有されている鍵情報202を用いて、まず暗号化された擬似乱数を復号する。次に、復号された擬似乱数を用いて、暗号化されたデジタル情報214を復号し、元のデジタル情報214を得る。本実施の形態の著作権保護システムは、デジタル情報を送信するとき、暗号化されているので、デジタル情報の不正な複製を防ぐことができ、著作権者の権利を保護することができる。

【0023】実施の形態4．前記実施の形態3では、第2の装置208及び第3の装置215において、共有の鍵情報202を保持していたが、デジタル情報214

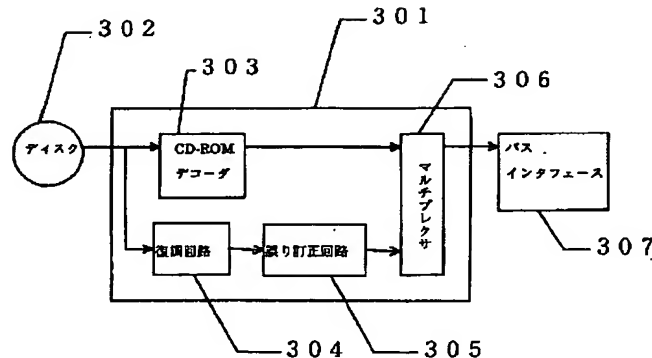
を送信するときのみ保持するようにし、送信が終了したら装置内から消去し、次の送信を開始するときに、再び共有するようにすることもできる。

【0024】実施の形態5. 前記実施の形態3では、鍵情報202を第2の装置208及び第3の装置215に送信するとき、初期値219を暗号化鍵としていたが、まず、最初の第1の装置201に対し、第2の装置208の保持する第2のID情報209および第3の装置215の保持する第3のID情報216を送信し、第1の装置201において、第1のID情報203と第2の装置208及び第3の装置215から送られてきた第2のID情報209及び第3のID情報216をもとに第1の装置201のみが保有している鍵情報202を秘密のパラメーターとして新たな暗号化鍵を暗号化鍵生成手段204において生成し、これを初期値219の代わりに用いることもできる。

【0025】実施の形態6. 前記実施の形態3では、鍵情報202を暗号化するために暗号化鍵生成手段205で生成した暗号化鍵は、第1の装置201、第2の装置208及び第3の装置215で保持されていたが、これら3つの装置のいずれかが、別の装置に入れ替わった場合は、次のようにすればよい。まず、第1のID情報203、第2のID情報209及び第3のID情報216を用いて、暗号化鍵生成手段204で新たな暗号化鍵を生成する。次に、生成された暗号化鍵を、第1の暗号化手段205で初期値219を暗号化鍵として暗号化し、第2の装置208及び第3の装置215に送信する。第2の装置208及び第3の装置215では初期値219を用いて復号し、暗号化鍵生成手段204で生成された新たな暗号化鍵は共有される。

* 30

【図3】



* 【0026】実施の形態7. 前記実施の形態1～6の著作権保護方法及び著作権保護システムは、DVD (Digital Video Disc)、CD-ROMなど、デジタル情報記録媒体全般の再生装置に用いることもできる。また、第1の装置201は、ICカードおよびPCカードなどの携帯型情報記録媒体としたが、鍵情報202を秘密に保持できる記録媒体であれば良い。

【0027】

【発明の効果】以上のように、本発明による著作権保護方法及び著作権保護システムは、デジタル情報の不正な複製を防ぐことができ、著作権者の権利を保護することができる効果がある。

【図面の簡単な説明】

【図1】 本発明の著作権保護方法を説明する図である。

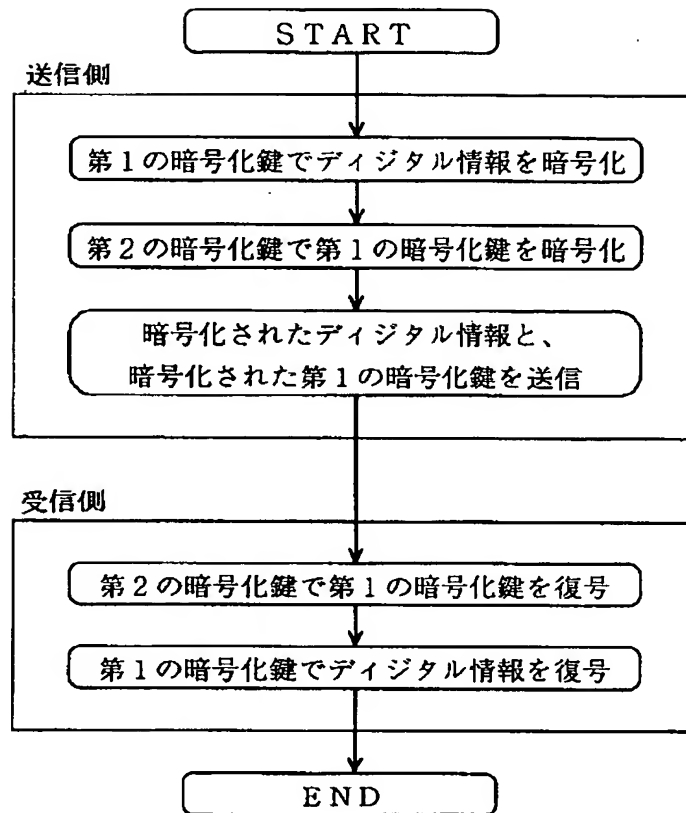
【図2】 本発明の著作権保護システムの構成図である。

【図3】 従来の光ディスクシステムの構成図である。

【符号の説明】

201 第1の装置、202 鍵情報、203 第1のID情報、204 暗号化鍵生成手段、205 第1の暗号化手段、206 第1の復号手段、207 第1のインタフェース、208 第2の装置、209 第2のID情報、210 擬似乱数生成手段、211 第2の暗号化手段、212 第2の復号手段、213 第2のインタフェース、214 デジタル情報、215 第3の装置、216 第3のID情報、217 第3の復号手段、218 第3のインタフェース、219 初期値。

【図 1】



【図2】

